



# Platforma RSA enVision

## Monitorowanie w czasie rzeczywistym

### Cel użytkownika

Systemy bezpieczeństwa sieciowego składają się z licznych rozwiązań generujących codziennie tysiące zdarzeń. Wydarzenia takie, jeśli są prawidłowo gromadzone i analizowane, mogą pomóc przedsiębiorstwu w ochronie przed zagrożeniami zarówno wewnętrznymi, jak i zewnętrznymi. Jednak aby stworzyć efektywne środowisko bezpieczeństwa, przedsiębiorstwo musi dysponować kompletnym obrazem wykorzystania swojej sieci.

Posiadając zainstalowany system przechwytyjący, gromadzący i chroniący wszystkie dane, przedsiębiorstwo może weryfikować zgodność z zasadami bezpieczeństwa, generować ostrzeżenia o możliwych naruszeniach zgodności oraz analizować i raportować wydajność sieci.

### Wykorzystanie i monitorowanie sieci

Firmy na całym świecie wykorzystują rozwiązania RSA enVision do radykalnej poprawy efektywności posiadanej infrastruktury bezpieczeństwa, w tym celu monitorując użycie wszystkich zasobów swoich sieci i zarządzając nim. Urządzenia RSA przechwytyją wszystkie dane ze wszystkich elementów infrastruktury sieciowej, co pozwala firmie uzyskać obraz całej sieci i połączyć szczegółową analizę bezpieczeństwa z potrzebami i wymaganiami operacyjnymi. Urządzenia Network Intelligence zapewniają bezpieczeństwo poprzez gromadzenie wszystkich danych (All the Data™) ze wszystkich elementów sieci, wykorzystując przy tym bazę danych protokołu internetowego Internet Protocol Database™ LogSmart® (IPDB). Dzięki temu firma może wizualizować stan sieci, śledzić przepustowość, określać wykorzystanie protokołu, wizualizować profile ruchu i generować raporty na temat użytkowania sieci. Mając do dyspozycji te wszystkie możliwości, można analizować dokładne informacje w celu wykorzystania do działań i planowania, zwiększyć dostępność sieci i usług oraz zapewnić natychmiastowe reagowanie tak, aby czas przestoju był jak najkrótszy.

W szczególności, baza danych LogSmart IPDB zapewnia trzy kluczowe elementy efektywnego śledzenia i monitorowania użycia sieci:

- Dostosowywanie do bazowego poziomu bezpieczeństwa (baselining) – poziom wykorzystania sieci jest wczesnym sygnałem wpływu, jaki na dostępność i jakość usług mogą mieć awarie lub incydenty związane z bezpieczeństwem. Rozwiązanie RSA enVision umożliwia stworzenie

poziomów bazowych dla zwyczajnego użytkownika, a przypadki użytkownika wykraczające poza takie poziomy są następnie analizowane w celu ustalenia, czy nastąpiło jakieś zdarzenie. Ważnymi atrybutami poziomów bazowych do wykorzystania i monitorowania sieci są:

- dane zbiorcze z interfejsów pokazujące, jaka ilość danych przepływa przez sieć,
- ruch według poszczególnych komputerów, użytkowników, grup i serwerów,
- profile ruchu według dostępu do usług (WWW, nazwy, pliki, P2P),
- podsumowanie i statystyka użycia protokołu IP: przepustowość, sesje,
- jakość usług: przepustowość, czas odpowiedzi i opóźnienie.

- Ostrzeżenie – administrator może skonfigurować ostrzeżenia tak, by były wyzwalane po przekroczeniu progów poziomów bazowych. Ostrzeżenia mogą być generowane po spełnieniu następujących istotnych kryteriów:

- przekroczenia szerokości pasma według działu/miejsca,
- przekroczenia liczby sesji według działu/miejsca,
- przekroczenia liczby aplikacji według działu/miejsca.

- Raportowanie i kontrola – rozwiązania RSA enVision zapewniają egzekwowanie odpowiedzialności dzięki funkcji tworzenia kompleksowych i dokładnych raportów, zarówno na żądanie, jak i zaplanowanych. Generują one reprezentacje graficzne takich kluczowych informacji, jak:

- okresy szczytowego nasilenia ruchu w danym czasie,
- potrzeby w zakresie wydajności zasobów.

### Baza danych protokołu internetowego firmy

Dzięki wykorzystaniu zaawansowanej architektury LogSmart IPDB stosowanej przez setki przedsiębiorstw na całym świecie, platforma enVision™ firmy Network Intelligence jest w stanie przechwytywać wszystkie dane („All the Data”) z sieci, mechanizmów zabezpieczających, hostów, warstw aplikacji i urządzeń do zapisu danych zainstalowanych w obrębie całego przedsiębiorstwa. Baza danych LogSmart IPDB umożliwia analizę danych zarówno w czasie rzeczywistym, jak i archiwalnych, oraz ich prezentację w formie przeglądów i raportów dostosowanych do różnorodnych potrzeb każdego działu przedsiębiorstwa – np. działu IT,





działu bezpieczeństwa, osób odpowiedzialnych za zapewnienie zgodności i zarządzanie ryzykiem czy wreszcie zarządu.

Zalety bazy danych LogSmart IPDB:

- Zaprojektowana w celu przechowywania i zapewnienia efektywnej pracy z wykorzystaniem danych nieusystematyzowanych, bez konieczności ich filtrowania lub normalizowania
- Zapewnia utrzymanie cyfrowego łańcucha ochrony danych, dzięki czemu dane raz wprowadzone do bazy nie mogą zostać zmienione – w odróżnieniu od większości schematów danych wykorzystywanych w rozwiązaniach opartych na RDBMS
- Nie są konieczne programy typu agent
- Rozproszona architektura typu „peer-to-peer” umożliwia dużą skalowalność i wydajność

## O firmie RSA enVision

Firma Network Intelligence, część RSA – oddziału firmy EMC zajmującego się bezpieczeństwem – jest uznanym na rynku liderem w przekształcaniu danych występujących w całej sieci przedsiębiorstwa na informacje bezpieczne i zgodne z przepisami. Baza danych LogSmart® Internet Protocol Database (IPDB)™ oferuje architekturę, która jako jedyna umożliwia efektywne gromadzenie i ochronę danych o kluczowym znaczeniu w działalności klientów. Dzięki firmie RSA setki klientów na całym świecie zapewniają sobie zgodność i bezpieczeństwo bez zwiększania kosztów i złożoności.

## Struktura działań związanych z bezpieczeństwem

Środowisko bezpieczeństwa			Cele zabezpieczeń		Środki:
Operacje na styku z internetem	Operacje e-commerce	Systemy i aplikacje wewnętrzne			
			<b>Wdrożenie kontroli dostępu</b>	<ul style="list-style-type: none"> <li>&gt; Monitorowanie uprzywilejowanych użytkowników</li> <li>&gt; Zgodność z zasadami korporacyjnymi</li> </ul>	<ul style="list-style-type: none"> <li>✓ Zarządzanie dziennikiem</li> <li>✓ Identyfikacja zasobów</li> <li>✓ Poziom bazowy</li> <li>✓ Raport i kontrola</li> <li>✓ Ostrzeżenie</li> <li>✓ Analiza przestępstw</li> <li>✓ Zarządzanie zdarzeniami</li> </ul>
			<b>Monitorowanie w czasie rzeczywistym</b>	<ul style="list-style-type: none"> <li>&gt; Diagnoza zdarzeń dotyczących sieci i zabezpieczeń</li> <li>&gt; „Co się dzieje?”</li> </ul>	
			<b>Zmniejszenie liczby błędnych klasyfikacji</b>	<ul style="list-style-type: none"> <li>&gt; Potwierdzanie ostrzeżeń systemu IDS</li> <li>&gt; Umożliwienie eskalacji krytycznych alertów</li> </ul>	
			<b>Skorelowane wykrywanie zagrożeń</b>	<ul style="list-style-type: none"> <li>&gt; Obserwacja sieci rozległych</li> <li>&gt; Konsolidacja rozproszonych ostrzeżeń IDS</li> </ul>	
			<b>Wdrażanie listy obserwacyjnej</b>	<ul style="list-style-type: none"> <li>&gt; Ryzyko zagrożeń zewnętrznych</li> <li>&gt; Dochodzenia wewnętrzne</li> </ul>	
			<b>Wykrywanie nieautoryzowanych usług sieciowych</b>	<ul style="list-style-type: none"> <li>&gt; Wyłączenie niedozwolonych usług</li> <li>&gt; Wpływ własności intelektualnej</li> </ul>	
			<b>Monitorowanie zgodności z SLA</b>	<ul style="list-style-type: none"> <li>&gt; Sprawdzenie wypełnienia umowy</li> <li>&gt; Monitorowanie względem poziomów bazowych</li> </ul>	



RSA Security Inc.  
RSA Security Ireland Limited  
[www.rsa.com](http://www.rsa.com)

The Security Division of EMC

© 2007 RSA Security Inc. Wszelkie prawa zastrzeżone.  
RSA, RSA Security, RSA Secured, SecurID, SecurCare oraz logo RSA są zastrzeżonymi znakami towarowymi lub znakami towarowymi firmy RSA Security Inc. w Stanach Zjednoczonych i/lub innych krajach. Microsoft i Windows są zastrzeżonymi znakami towarowymi lub znakami towarowymi firmy Microsoft Corporation w Stanach Zjednoczonych i/lub innych krajach. EMC jest zastrzeżonym znakiem towarowym EMC Corporation. Wszystkie inne produkty i usługi wymienione w niniejszej publikacji są znakami towarowymi odpowiednich podmiotów.